

Re: PKI and Relying Parties

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2002-03/0655.html>

From: Anne & Lynn Wheeler (lynn@garlic.com)

Date: 03/29/02

From: Anne & Lynn Wheeler <lynn@garlic.com>

Date: Fri, 29 Mar 2002 13:16:18 GMT

john.veldhuis@universal.nl writes:

- > *CRLs for certain certificates are usually signed by the CA who has*
- > *certified them.*
- > *So, one way or another, someone has to perform CA duty.*

If you have a PKI with certificates. For a relying party only environment, it is possible to have a pki, or a npki, or a spki ... that doesn't have certificates ... just an online environment.

In effect, certificates are something like letters of credit from the (offline) sailing ship days (where there was no way of calling up and verifying the information) or the plastic payment cards before online transactions (the cards look the same, but instead of using the front for offline transactions, the magstripe on the back is used for online transactions).

the certificates are somewhat like processor cache lines ... so the processor can use the local information w/o having to reference the original information. CRLs are analogous to the cache-line broadcast invalidation signals (you hope that everybody that needs to get the signal, is listening).

In the case of SSL domain name certificates ... it could be possible for the relying part to provide the domain name and get back both an ip address and an associated public key from the domain name infrastructure (no certificates, just online information, both the ip-address and the public key).

First, public keys aren't currently registered with the domain name ... so while the domain name infrastructure has the capability of serving up arbitrary information (not just ip-addresses), it doesn't currently have the public key information to server up.

Second, there are integrity issues with the domain name infrastructure serving ... which effectively has given rise to the whole SSL domain name certificates. A server someplace applies to a certification authority to get them to certify a credential as to the server's

domain name.

Now a certification authority typically is just that ... they certify information ... they aren't the authoritative agency responsible for the information they are certifying. A certification authority typically checks out the information they are certifying with the authoritative agency that is responsible for the information being certified.

So who is the authoritative agency for domain name information?, the domain name infrastructure. This is the same domain name infrastructure that supposedly has integrity issues giving rise to the justification for SSL domain name certificates. So one of the solutions to address the integrity issues on behalf of certification authorities ... is to have public keys registered with the domain name infrastructure at the same time a domain name is registered. That registered public key, used in various domain name infrastructure business operations addresses various domain name infrastructure integrity issues.

So if domain name infrastructure integrity issues are addressed, it goes a long way to eliminating the original requirement for having SSL domain name certificates. Also if that approach includes the registering of public keys, then the domain name infrastructure now has public keys that it can serve up real-time at the same time it serves up ip-addresses (as per "one").

In the case of relying-party-only financial operations, they can be their own CA. Note however, this typically involves registering a public key for an account, generating a certificate (typically with account number, public key and nothing else, in part because of privacy & liability issues), saving the certificate original in the account record, and sending a copy of the certificate back to the public key owner.

The public key owner (also the account owner) then generates some form of transactions which they then sign with their private key. They then package up the transaction, the digital signature, and the certificate copy back to their financial institution (relying party). Both the transaction and the certificate contain the account number (redundant information), which then instructs the processing to retrieve the account record.

now, the account record contains the original of the certificate, a copy of which is also appended to the transaction. It is at this point that it is apparent that the appending of the copy of a certificate to the end of a transactions is redundant and superfluous ... because it is being sent back to the relying-party which has the original of the certificate ... which the relying-party is going to read as part of processing the transaction.

Now, for various efficiency reasons, the relying-party when it generates the certificate (ASN.1 encoded) is likely to store the unencoded version of the fields in the account record (and/or the unencoded version of the fields are already going to be in the account record). As a result, the relying-party is retrieving the same information from the account record (as might be found in the certificate) ... but already in unencoded and directly useable form.

The other issues that arises in the financial relying-party only scenario is one of service. The reason that the original of the certificate (or at least all the same information in directly useable, unencoded form) is stored in the account record ... is when somebody calls up with a question or some issue as to why something works or doesn't work with their account ... all that information is directly available to answer the call.

A financial relying-party is also likely to prefer real-time copies of the information and a paradigm designed for online, real-time operation ... as opposed to a paradigm designed for offline, stale information operation ... especially when it is performing online, real-time operations; aka certificates are redundant and superfluous and were never intended as a solution to online, relying-party-only operation in the first place.

random refs:

<http://www.garlic.com/~lynn/subtopic.html#privacy> privacy, reliability, relying-party-only

<http://www.garlic.com/~lynn/subtopic.html#sslcerts> ssl certification

<http://www.garlic.com/~lynn/subtopic.html#radius> various online certificate-less pki

--

Anne & Lynn Wheeler | lynn@garlic.com, <http://www.garlic.com/~lynn/>

- *Next message:* [Florian Konnertz: "Re: newbie – scp: stderr i.n.a tty, broken pipe error"](#)
- *Previous message:* [Nico Kadel-Garcia: "Re: newbie – scp: stderr i.n.a tty, broken pipe error"](#)
- *In reply to:* [john.veldhuis@universal.nl: "Re: PKI and Relying Parties"](#)
- *Next in thread:* [Citizen Fish: "Re: PKI and Relying Parties"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)